



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Peter Szor

Assignee: Symantec Corporation

Title: KERNEL MODE OVERFLOW ATTACK PREVENTION SYSTEM AND

METHOD

10/781,207

Examiner: Unknown

Group Art 2182

Unit:

Filed:

Docket No.: SYMC1048

Serial No.:

Monterey, CA May 25, 2004

February 17, 2004

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner.

U.S. PATENT DOCUMENTS

•	DOCUMENT NUMBER	DATE	NAME
1)	5,696,822	12/09/97	Nachenberg
2)	5,822,517	10/13/98	Dotan
3)	6,301,699	10/09/01	Hollander et al.
4)	6,357,008	03/12/02	Nachenberg

OTHER DOCUMENTS

1)	Szor, P., U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
2)	Szor, P., U.S. Patent Application Serial No. 10/371,945, filed February 21, 2003, entitled "SAFE MEMORY SCANNING".

GUNNISON, McKAY & HODGSON, L.L.P. 1900 Garden Road Montercy, CA 93940 (831) 655-0880 Fax (831) 655-0888

Serial No. 10/781,207



3)	Szor, P., U.S. Patent Application Serial No. 10/464,091, filed June 17, 2003, entitled "SEND BLOCKING SYSTEM AND METHOD".
4)	Szor, P., U.S. Patent Application Serial No. 10/611,472, filed June 30, 2003, entitled "SIGNATURE EXTRACTION SYSTEM AND METHOD".
5)	Szor, P., U.S. Patent Application Serial No. 10/681,623, filed October 7, 2003, entitled "UNMAPPED CODE BLOCKING SYSTEM AND METHOD".
6)	Szor, P., <i>"Attacks on WIN32"</i> , Virus Bulletin Conference, October 1998, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 57-84.
7)	Szor, P., "Memory Scanning Under Windows NT", Virus Bulletin Conference, September 1999, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-22.
8)	Szor, P., "Attacks on WIN32-Part II", Virus Bulletin Conference, September 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 47-68.
9)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
10)	Buysse, J., "Virtual Memory: Windows NT® Implementation", pp. 1-15 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://people.msoe.edu/~barnicks/courses/cs384/papers19992000/buyssej-Term.pdf.
11)	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:www.windowslibrary.com/Content/356/06/2.html.
12)	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/kernekmode.asp. No author provided.
13)	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved April 16, 2003. Retrieved from the internet: URL:http://www.entercept.com/products/technology/interception.asp. No author provided.
14)	Kath, R., "The Virtual-Memory Manager in Windows NT", pp. 1-11 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/dngenlib/html/msdn_ntvmm.asp?frame=true.
15)	Szor, P. and Kaspersky, E., "The Evolution of 32-Bit Windows Viruses", Windows & .NET Magazine, pp. 1-4 [online]. Retrieved on April 16, 2003. Retrieved from the internet: URL:http://www.winnetmag.com/Articles/Print.cfm?ArticleID=8773.
16)	Szor, P., "The New 32-bit Medusa", Virus Bulletin, December 2000, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 8-10.

17)	Szor, P., <i>"Shelling Out"</i> , Virus Bulletin, February 1997, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 6-7.
18)	McCorkendale, B. and Szor, P., "Code Red Buffer Overflow", Virus Bulleting, September 2001, Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, England, pp. 4-5.
19)	Nachenberg, C., "A New Technique for Detecting Polymorphic Computer Viruses", University of California, Los Angeles, 1995.
20)	"INFO: CreateFileMapping() SEC_* Flags", pp.1-2 [online]. Retrieved on September 24, 2003. Retrieved from the internet: URL:http://support.microsoft.com/default.aspx?scid=http://support. microsoft.com:80/support/kb/articles/Q108/2/31.asp&NoWebContent=1. No author provided.
21)	"CreateFileMapping", pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the internet: URL:http://msdn.microsoft.com/library/en-us/fileio/base/createfile mapping.asp?frame=true. No author provided.

A PTO form 1449 listing these documents is enclosed.

Citation of the above documents shall not be construed as:

- 1. an admission that the documents are necessarily prior art with respect to the instant invention;
- 2. a representation that a search has been made, other than as described above; or
- 3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in $\S 1.56(b)$.

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail it an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 25, 2004.

Attorney for Applicant(s)

May 25, 2004
Date of Signature

Serge J. Hodgson

Attorney for Applicant(s)

Respectfully submitted,

Reg. No. 40,017

(831) 655-0880

									Sheet	1 of 7
Form PTC	-1449	MATION DISCLOSUI IN AN APPLICAT several sheets if			Atty Docke	No.		Se	erial No.	
E					SYMC1048 10/781,207					
S E 10	IMFORM	MATION DISCLOSU	RE CITATION	г	Applicant(s)				
~ 188		IN AN APPLICA	rion		Peter Sz	or				
MIZ) A				Filing Date	9		Gı	roup	
A	N Use	several sheets if	necessary)		February	17, 2004		2	182	
TENTA			υ.s.	PATENT I	OCUMENTS					
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	•	CLASS	SUBCLAS	s	FILING D IF APPRO	
	AA	5,696,822	12/09/97	Nachenb	erg	380	4			
	AB	5,822,517	10/13/98	Dotan		395	186			
	AC	6,301,699	10/09/01	Holland	er et al.	717	4			
	AD	6,357,008	03/12/02	Nachenb	berg 713		200			
	AE									
	AF									
•	AG									
	AH			!						
	AI									
	AJ									
	AK									
			FOREI	ON PATENT	DOCUMENTS	5				
	.					· · · · · · · · · · · · · · · · · · ·			Trans	lation
	<u> </u>	DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	s	YES	NO
	AL									
	AM									
	AN						_			
	AO									
-	AP									
		OTHER DOCUMEN	TS (Includin	g Author,	Title, Date,	Pertinent P	Pages, Etc	c.)		
•	AR	Szor, P., U.S. 2003, entitled						ile	ed Febru	ary 6,
	AS	Szor, P., U.S. 2003, entitled	Patent Ap NSAFE MEM	plication ORY SCAND	n Serial N NING".	0. 10/371	,945, f	ile	ed Febru	ary 21,
	AT	Szor, P., U.S. 2003, entitled					,091, f	ile	ed June	17,

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Date Considered

Examiner

Form PTO	Form PTO-1449				Atty Docket No.			Serial No.		
					SYMC1048 10/781,207					
:	INFOR	MATION DISCLOS	URE CITATIO	N	Applicant(s)					
		IN AN APPLIC	ATION		Peter Szor					
						:e		Group		
	(Use several sheets if necessary)					17, 2004		2182		
			υ.s.	. PATENT I	OCUMENTS					
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS	S FILING IF APPR	DATE OPRIATE	
	AA								-	
	AB									
	AC									
	AD									
	AE									
	AF									
	AG				,					
	AH									
	AI		<u> </u>							
	AJ		-							
	AK									
	1	<u>.</u>	FOREI	GN PATENT	DOCUMENT	'S	1			
						.,		Tran	slation	
1.		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	NO	
	AL									
	AM			-			-	-		
	AN	 ·· .								
	AO									
	AP	 	 					_		
	l Ar	OTHER DOCUME	NTC / Tagludia	na Author /	Title Date	Postinost I	l Etc	- \		
	A.D.								3.0	
	AR	Szor, P., U.S 2003, entitle	d "SIGNATUR	E EXTRACT	Serial No ION SYSTE	M AND METH	OD".	red June	30,	
	AS	Szor, P., U.S 2003, entitle						led Octob	er 7,	
	AT	Szor, P., "At Bulletin Ltd,	tacks on WII	N32", Vir	us Bullet don, Oxfo	in Confere rdshire, E	nce, Oc ngland,	tober 199 pp. 57-8	8, Virus	
Examiner			Date Consid	dered						
through ci	EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).									

Form PTO	Form PTO-1449				Atty Docket No. SYMC1048			Serial No. 10/781,207			
]	NFOR	MATION DISCLOS	URE CITATIO	N	Applicant(s) Peter Szor						
		IN AN APPLIC	ATION								
						te		Group			
	(Use several sheets if necessary)					7 17, 2004		2182			
			v.s	. PATENT I	DOCUMENTS						
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS	J	FILING DATE IF APPROPRIATE		
	AA										
	AB										
	AC										
	AD										
	AE				_						
	AF										
	AG										
	AH										
	AI										
	AJ										
	AK										
		<u> </u>	FOREI	GN PATENT	DOCUMENT	:s	1				
Translati							nslation				
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	ио		
	AL										
	AM										
	AN										
	AO										
	AP										
		OTHER DOCUME	NTS (Includi	ng Author,	Title, Date,	, Pertinent F	ages, Etc	;.)			
·	AR	Szor, P., "M September 19 England, pp.	99, Virus Bu	ing Under ulletin Lt	Windows I	<i>NT"</i> , Virus entagon, A	Bullet: bingdon	in Confe , Oxford	rence, shire,		
	AS	Szor, P., "A 2000, Virus I 47-68.	ttacks on W. Bulletin Ltd	IN32-Part d, The Per	<i>II"</i> , Virantagon, Al	us Bulletin bingdon, O	n Confe xfordsh	rence, S ire, Eng	eptember land, pp.		
	AT	Chien, E. and Buffer-Overf September 20 England, pp.	low Techniqu 02, Virus Bu	ues In Cor	mputer Vi:	ruses", Vi	rus Bull	letin Co	nference,		
Examiner			Date Consi	dered							
EXAMINER: through ci	Initia tation	al if reference c if not in confor	onsidered, whe	ther or not	citation is	s in conforma	nce with	MPEP 609; next comm	draw line		

to applicant(s).

Form PTC	Form PTO-1449					et No.		Serial No.			
					SYMC1048 10/781,207						
:	INFOR	MATION DISCLOS	JRE CITATIO	N	Applicant(s) Peter Szor						
		IN AN APPLICA	ATION								
					Filing Dat	te		Group			
	(Use	several sheets i	f necessary)		February	7 17, 2004	<u> </u>	2182			
			U.S	. PATENT	DOCUMENTS						
EXAMINER INITIAL		DOCUMENT NUMBER DATE			CLASS		SUBCLASS	FILING DATE IF APPROPRIATE			
	AA										
	AB								*		
	AC										
	AD				••	-					
	AE										
	AF			"							
	AC										
	AH			1							
	AI										
	AJ										
	AK										
	<u> </u>		FORE	GN PATENT	DOCUMENT	'S					
								Tran	slation		
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLASS	YES	мо		
	AL	,					-				
	AM										
	AN						-				
-	AO				,						
	AP										
	1	OTHER DOCUME	NTS (Includi	ing Author,	Title, Date	Pertinent l	l Pages, Etc	 .)			
•	AR	·									
	120	Buysse, J., Some continuous formula and second continuous formula	rieved on	April 16,	2003. Ref	trieved fr	om the i	nternet:	ouyssej-		
	AS	Dabak, P., Bo pp. 1-8 [onli URL:http://ww	ne]. Retri	eved on Ap	oril 16, 3	2003. Retr	ieved fr	System Se om the i	ervices", nternet:		
	AT	"How Entercep Retrieved on URL:http://ww provided.	April 16,	2003. Ret	rieved fro	om the int	ernet:				
Examiner			Date Consi	dered							
EXAMINER: through ci to applica	tation	al if reference co if not in conform	onsidered, whe	ether or not considered.	citation is Include co	s in conforma	ance with torm with	MPEP 609; onext commun	draw line nication		

Form PTC	Form PTO-1449			Atty Docks	et No.		Serial No.			
					SYMC1048 10/781,207					
	INFOR	MATION DISCLOS	JRE CITATIO	N	Applicant(s) Peter Szor					
		IN AN APPLIC	ATION							
					Filing Da	te		Group		
	(Us	e several sheets i	f necessary)		February	7 17, 2004		2182		
			U. S	. PATENT	DOCUMENTS					
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS		DATE PROPRIATE	
	AA									
	AB									
	AC									
	AD									
•	AE									
	AF									
•	AG									
	AH									
	AI									
	AJ									
	AK									
			FORE	IGN PATENT	DOCUMENT	rs				
								Tra	nslation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	ио	
	AL									
	AM									
	AN									
	AO	-								
	AP									
		OTHER DOCUME	NTS (Includ	ing Author,	Title, Date	, Pertinent .	Pages, Etc	z.)	•	
•	AR	"How Entercep Retrieved Apr URL:http://ww provided.	il 16, 2003	3. Retriev	ed from t	he interne	et:			
	AS	Kath, R., "Th Retrieved on URL:http://ms asp?frame=tru	April 16, 2 dn.microsof	2003. Retr	ieved fro	m the inte	ernet:			
E	АТ	Szor, P. and Windows & .NE Retrieved fro URL:http://ww	Γ Magazine, m the inter	pp. 1-4	[online].	Retrieved	d on Apr	il 16, 2	es", 1003.	
Examiner	:		Date Consi	idered						
EXAMINER: through ci	itatio	ial if reference con if not in conform								

Form PTO	Form PTO-1449				Atty Docke		Serial No. 10/781,207			
	NTPODA	MATION DISCLOS	מסק מידים	NT.	Applicant(s) Peter Szor					
	INFORD	IN AN APPLIC		/11						
		IN AN APPUIC	AIION		Filing Date Group					
	(1100	several sheets i	f negeggary)			7 17, 2004		2182		
	1056	Beverar Bheets 1	<u></u>	. PATENT 1						
EXAMINER				1				FILING	DATE	
INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS		OPRIATE	
	AA									
	AB									
	AC									
	AD									
	AE									
	AF									
	AG									
	AH									
	AI									
	АJ									
	AK	,								
			FORE	IGN PATENT	DOCUMENT					
								Trans	slation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	YES	NO	
	AL									
	AM	**								
	AN								·	
-	AO			1				-		
	AP									
`		OTHER DOCUM	NTS (Includ	ing Author. '	Title. Date	Pertinent F	Pages Etc		. L	
•	AR	Szor, P., "T. Bulletin Ltd	he New 32-b	it Medusa	", Virus 1	Bulletin,	December	2000, V	irus 0.	
	AS	Szor, P., "S. Ltd, The Pen	helling Out tagon, Abin	", Virus I gdon, Oxfo	Bulletin, ordshire,	February England,	1997, Vi pp. 6-7	rus Bull	etin	
	АТ	McCorkendale September 20 England, pp.	01, Virus B							
Examiner			Date Consi	dered						
through ci	EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).									

Form PTO	Form PTO-1449			Atty Docke	•					
					SYMC1048 10/781,207					
:	INFOR	MATION DISCLOST	RE CITATIO	N	Applicant(s)					
		IN AN APPLICA	TION		Peter Sz	or				
D.						:e		Group		
	(Use	several sheets if	necessary)		February	17, 2004		2182		
			U.S	. PATENT I	OCUMENTS					
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLASS		DATE ROPRIATE	
	AA									
	AB									
	AC									
	AD									
	AE									
	AF									
	AG									
	AH									
	AI				"					
	AJ								·	
	AK						 			
			FOREI	GN PATENT	DOCUMENT	S				
								Tran	slation	
		DOCUMENT NUMBER	DATE	COUNTRY	 	CLASS	SUBCLASS		NO	
	AL									
-	AM									
	AN									
	AO									
4	AP									
•		OTHER DOCUME	NTS (Ingludi	ng Author '	Title Date	Portinent	Dages Fto	<u> </u>		
•	AR	Nachenberg, C. Viruses", Univ	, "A New T	echnique	for Detec	ting Polyn	morphic			
	AS	"INFO: CreateR September 24, URL:http://sup com:80/support	2003. Retroport.micro	ieved from soft.com/	m the into	ernet: spx?scid=l	nttp://s	upport.m	icrosoft.	
	AT	"CreateFileMar Retrieved from URL:http://msd asp?frame=true	the inter	net: t.com/lib	rary/en-u					
Examiner			Date Consi	dered						
		al if reference co if not in conform								